|  |  |
| --- | --- |
| 3GPP TR 33.866 V0.4.0 (2021-03) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2;  (Release 17) | |
|  | |
| *5G-logo_175px* | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview of eNA 8

5 Key issues 8

5.1 Key issues related to securing the data provided to any type of analytics function 9

5.1.1 Key Issue #1.1:Integrity protection of data transferred between AF and NWDAF 9

5.1.1.1 Key issue details 9

5.1.1.2 Security Threats 9

5.1.1.3 Potential Requirements 9

5.1.2 Key Issue #1.2: Processing of tampered data 9

5.1.2.1 Key issue details 9

5.1.2.2 Security threats 9

5.1.2.3 Potential security requirements 10

5.1.3 Key Issue #1.3: Authorization of NF Service Consumers for data access via DCCF 10

5.1.3.1 Key issue details 10

5.1.3.2 Security threats 10

5.1.3.3 Potential security requirements 11

5.1.4 Key Issue #1.4: Security protection of data via Messaging Framework 11

5.1.4.1 Key issue details 11

5.1.4.2 Threats 12

5.1.4.3 Potential security requirements 12

5.1.5 Key Issue #1.5: UE data collection protection at NF/NWDAF 12

5.1.5.1 Key issue details 12

5.1.5.2 Security threats 12

5.1.5.3 Potential security requirements 13

5.2 Key issues related to detection of cyber-attacks and anomaly events by analytics function 13

5.2.1 Key Issue #2.1: Cyber-attacks detection supported by NWDAF 13

5.2.1.1 Key issue details 13

5.2.1.2 Security threats 13

5.2.1.3 Potential security requirements 13

5.2.2 Key Issue #2.2: Anomalous NF behaviour detection by NWDAF 14

5.2.2.1 Key issue details 14

5.2.2.2 Security threats 14

5.2.2.3 Potential security requirements 14

5.3 Key issues related to data transfer protection 14

5.3.1 Key Issue #3.1: Privacy preservation for transmitted data between multiple NWDAF instances 14

5.3.1.1 Key issue details 14

5.3.1.2 Security threats 15

5.3.1.3 Potential security requirements 15

5.3.2 Key Issue #3.2: Protection of UE data in transit 15

5.3.2.1 Key issue details 15

5.3.2.2 Security Threats 15

5.3.2.3 Potential security requirements 15

5.3.3 Key Issue #3.3: Ensuring restrictive transfer of ML models between authorized NWDAF instances 15

5.3.3.1 Key issue details 15

5.3.3.2 Security Threats 15

5.3.3.3 Potential security requirements 16

6 Solutions 16

6.0 Mapping of solutions to key issues 16

6.1 Solution #1: UE data collection protection 17

6.1.1 Introduction 17

6.1.2 Solution details 17

6.1.3 Evaluation 17

6.2 Solution #2: Network Analysis Framework for DDoS Attack 17

6.2.1 Introduction 17

6.2.2 Solution details 17

6.2.2.1 Introduction 17

6.2.2.2 Network Analysis Framework for DDoS attack 18

6.2.3 Evaluation 18

6.3 Solution #3: Usage of current SBA mechanisms to protect data in transit 19

6.3.1 Introduction 19

6.3.2 Solution details 19

6.3.3 Evaluation 19

6.4 Solution #4: DCCF determining if NF Service consumer is authorized to invoke a service to a Data Producer NF for data collection 19

6.4.1 Introduction 19

6.4.2 Solution details 19

6.4.2.1 Detailed Procedure 21

6.4.3 Evaluation 22

6.5 Solution #5: Providing the Security protection of data via Messaging Framework 22

6.5.1 Introduction 22

6.5.2 Solution details 23

6.5.2.1 DCCF initiated key refresh procedure 25

6.5.3 Evaluation 26

6.6 Solution #6: Integrity protection of data transferred between AF and NWDAF 26

6.6.1 Introduction 26

6.6.2 Solution details 26

6.6.3 Evaluation 26

6.7 Solution#7: Detection of anomalous NF behaviour by NWDAF 26

6.7.1 Introduction 26

6.7.2 Solution details 26

6.7.3 Evaluation 28

6.8 Solution#8: Privacy preservation of transmitted data 28

6.8.1 Introduction 29

6.8.2 Solution details 29

6.8.3 Evaluation 30

7 Conclusions 30

Annex A (informative): Change history 30

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document will study the security aspects of enablers for network automation for the 5G system based on the outcome of TR 23.700-91 [1]. More specifically, this study will identify security issues, requirements and corresponding potential security solutions related to the following objectives:

- UE data collection protection to fulfil the NWDAF functionalities including privacy consideration, data authenticity, data integrity, and accessibility aspects requirements.

- Detection of cyber-attacks and anomaly events supported by NWDAF and its related functions, specifically to identify parameters provided by UE and NFs, which can help to detect attacks and abnormal behaviours;

- Protection of data transferring (e.g. privacy consideration) in the inter-NWDAF/NWDAF instances.

NOTE: The user consent for UE data collection is not addressed in the present document, it will be discussed in TR 33.867 [2].

Editor's Note: This study is not complete until the user consent aspects in TR 33.867 that are applicable to eNA are finalized. How TR 33.867 conducts the user consent study (in a general way applicable to eNA or including specific aspects of eNA) will be discussed and addressed in the FS\_UC3S.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 23.700-91: "Study on enablers for network automation for the 5G System (5GS); Phase 2".

[2] 3GPP TS 33.867: "Study on user consent for 3GPP services".

[3] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[4] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services ".

[5] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[6] Draft NISTIR 8269: "A Taxonomy and Terminology of Adversarial Machine Learning"; <https://doi.org/10.6028/NIST.IR.8269-draft>

[7] ETSI SAI: "AI Threat Ontology"; <https://docbox.etsi.org/ISG/SAI/70-DRAFT/001/SAI-001v008.docx>.

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] 3GPP TR 28.809: "Study on enhancement of management data analytics".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [3] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [3].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [3] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [3].

AF Application Function

DoS Denial of Service

DDoS Distributed Denial of Service

eNA enablers for Network Automation

MDAS Management Data Analytics Service

MitM Man in the Middle

ML Machine Learning

NWDAF Network Data Analytics Function

OAM Operation, Administration and Maintenance

# 4 Overview of eNA

Editor's Note: This clause will contain a brief overview on eNA based on SA2's study (TR 23.700-91), including architectural assumptions, etc.

3GPP TS 23.288 [4] provides the Stage 2 architecture enhancements for 5G System (5GS) to support network data analytics services in 5G Core network, which forms the baseline for the present study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS).

The Network Data Analytics Function (NWDAF) as specified in 3GPP TS 23.501 [5] interacts with different entities within 5GS for data collection based on subscription to events, retrieval of information from data repositories, retrieval of information about NFs (e.g. from NRF for NF-related information) and on demand provision of analytics to consumers. The NWDAF provides analytics to 5GC NFs and OAM. Analytics information are either statistical information of the past events, or predictive information.

3GPP TR 23.700-91 [1] is an architectural study on enhancements for analytics and NWDAF, for which any security impact will be documented in the present document. This is in particular security impact for UE data collection protection, detection of cyber-attacks and anomaly events supported by NWDAF and its related functions, on protection of data transferring in the inter-NWDAF/NWDAF instances.

# 5 Key issues

Editor's Note: This clause contains all the key issues identified during the study.

## 5.1 Key issues related to securing the data provided to any type of analytics function

Editor's Note: This clause is for key issues on UE data collection protection to fulfil the NWDAF functionalities including privacy consideration, data authenticity, data integrity, accessibility aspects requirements, according to the first objective of the SID.

### 5.1.1 Key Issue #1.1:Integrity protection of data transferred between AF and NWDAF

### 5.1.1.1 Key issue details

The 5GS supports the collection and utilisation of the UE data and provide it to the NWDAF as an input to generate the analytic information (to be consumed by other NF).

As per KI#8 in TR 23.700-91 [1], there is no direct interface between the UE and the NWDAF. When AF is used for the communication between the NWDAF and UE for data collection, there is a need to study the security aspects for the data provided by the UE to NWDAF via AF and vice versa.

This key issue studies the integrity aspects on data collection and utilization of UE data in order to derive the analytics.

### 5.1.1.2 Security Threats

If the data shared between AF and NWDAF is not secured, it may lead to following issue;

Data can be modified and replayed by any unauthorized parties.

### 5.1.1.3 Potential Requirements

Integrity and replay protection shall be supported on the interface between AF and NWDAF for the UE data collection.

### 5.1.2 Key Issue #1.2: Processing of tampered data

#### 5.1.2.1 Key issue details

5GS is using ML to an increasing extend. NWDAF (TS 23.288 [4]) in 5GC and MDAS (TR 28.809 [9]) on OAM are two centralized frameworks currently responsible for ML-based analytics, e.g. abnormal behavior analytics. Furthermore, AI/ML is decentralized used in several use cases, such as efficiency optimization in RAN. Furthermore, a new data collection framework DCCF (clause 6.9, TR 23.700-91 [1]) is proposed for Rel-17.

Network data analytics is including the following steps:

* Request of analytics by consumer
* Collection of data by analytics function
* Processing of collected data by analytics function
* Reply analytics output to consumer by analytics function

While 3GPP provides sound security on network level, the data used by AI/ML is not being subject to security controls. This key issue seeks solutions countering a number of attacks against a 5GS involving tampered data.

#### 5.1.2.2 Security threats

Editor's Note: Threats need to be revisited if in line with NIST 8269 [6] and ETSI SAI [7] terminology.

Data used by AI/ML is not being subject to security controls. This allows for a number of attacks against a 5GS with severe impact on performance up to denial of service (DoS) conditions:

* **Adversarial examples** are generated by slightly perturbating input data. The data is perturbated in a space in which AI/ML algorithms are sensitive to change, leading to severe performance degradation and misclassifications in the inference process. This attack is well-known in human-centric use cases, such as image/audio classification.
* During training, tampered training data can lead to **model skewing**. Skewed models will provide false results in inference.
* Tampered data may also lead **information disclosure** by the inference of confidential/proprietary AI/ML algorithms.
* In more **simple attacks**, perturbations may not be slight (as those generated by adversarial example methods). In non-human-centric use cases (as most are in 5GS), the perturbations may just be false data to force misinterpretation.

Unprotected analytic functions are subject to:

* Decreased efficiency, e.g. power consumption, load balancing, QoS optimization
* System failure (DoS scenario)
* Inference of confidential ML algorithms employed by 5GS
* Leakage of privacy-related data derived from AI/ML models

#### 5.1.2.3 Potential security requirements

A 5GS analytics function shall be protected from processing unsanitized or tampered data.

### 5.1.3 Key Issue #1.3: Authorization of NF Service Consumers for data access via DCCF

#### 5.1.3.1 Key issue details

A Data Collection Coordination Function (DCCF) is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s). DCCF and Data Repository Function (DRF) can be standalone NFs, possibly co-located with NWDAF, or can be hosted by NWDAF. Data Collection notification to one or more Consumer NF(s) may be supported via a Messaging Framework. Adaptors supporting 3GPP services allow NFs to interact with the Messaging Framework. Only the interface between 3GPP entities and the adaptors is under 3GPP scope. This includes 3GPP services offered by adaptors to allow NFs to interact with the Messaging Framework.

TR 23.700-91-100 conclusion mentions that "Additional authorization for Consumers to access data from a Data Source via the DCCF and to access data from DRF (directly or via DCCF) needs to be coordinated with SA3". According to SA2 KI#11 conclusions, if a consumer subscribes to analytics notifications to the DCCF, the DCCF can subscribe itself to the data source and notify the data source that notifications are directly to be sent to the consumer. The data source will then send notifications to the consumer via the MF or via the DCCF.

This key issue addresses the authorization of data consumer to access the data (via DCCF) from the data source or the DRF, and the authorization aspects of the DCCF being allowed to subscribe the data on behalf of the consumer at the data source or the DRF, i.e. the security aspect on usage subscription/notification mechanisms for a consumer to receive notifications on a different path (as adapted in SA2 conclusions) will be studied.

#### 5.1.3.2 Security threats

DCCF introduces a new path for a NF Service Consumer (NFc) to access the data from data sources or a NF Service Producer (NFp). Due to the introduction of DCCF between consumer and producer, the existing security mechanism will not be sufficient, and the following threats needs to be addressed:

An unauthorized data consumer could request service from the DCCF.

NOTE: This threat can be addressed by existing SBA mechanisms. Therefore, no related requirement is added.

Based on a request from a DCCF, the Messaging Framework may provide data from a producer to a requesting data consumer, even though the consumer is not authorized to receive this data.

Based on a request from a DCCF data received from a data producer is stored in the DRF. When the data are later retrieved, the DCCF may provide the stored data to a non-authorized consumer if requested.

A DCCF could subscribe for data from the data source on behalf of data consumer without the data consumer authorizing DCCF to do so.

The data producer may be unable to correctly verify the identity of the data consumer since the data request is coming from DCCF on behalf of the consumer.

#### 5.1.3.3 Potential security requirements

The data consumer shall be authorized to access the data from the data source.

Authorization of the DCCF shall be supported to access a service of a data source on behalf of a data consumer.

Editor’s Note: Whether the service request including the URI, service name, etc., needs to be verified by the data source is FFS.

### 5.1.4 Key Issue #1.4: Security protection of data via Messaging Framework

#### 5.1.4.1 Key issue details

In [1], in the conclusions for the Key Issue #11 ‘Increasing efficiency of data collection’, DCCF (Data Collection Coordination Function) is defined for efficient data collection in 5GS. The DCCF is a control-plane function that coordinates data collection and triggers data delivery to Data Consumers.

TR 23.700-91 [1] lists several agreed principles for normative work, some of which are as follows:

- "When a Data Collection Coordination Functionality (DCCF) is deployed, it is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s)."

- "Data Collection notification to one or more Consumer NF(s) may be supported via a Messaging Framework. Adaptors supporting 3GPP services allow NFs to interact with the Messaging Framework.

- Data Collection notifications may also be supported directly from data provider to one or more Consumer NF(s), or via DCCF and not via the Messaging Framework.

NOTE 2: The Messaging Framework is outside the scope of 3GPP. Adaptors are not expected to be standardized by 3GPP, only the interface between 3GPP entities and the adaptors is under 3GPP scope. This includes 3GPP services offered by adaptors to allow NFs to interact with the Messaging Framework."

- "The DCCF coordinates data collection so the same data is not requested multiple times from the same data source."

The Messaging Framework is not expected to be standardized by 3GPP. It contains Messaging Infrastructure that propagates event information and data (e.g.: streaming and notifications) from data sources to data consumers. A Data consumer that uses the Data Management Framework sends requests to the DCCF rather than to a data producer.

Data notifications from data sources go through the adaptor on producer side, 3PA, the Messaging framework and the adaptor on consumer side, 3CA. The adaptor 3PA recognizes notifications from a Data Source and delivers them to the Messaging Framework. The adaptor 3CA obtains data from the Messaging Framework and send notifications to the Data Consumer. 3CA can condense multiple notifications into a single notification.

In TR 23.700-91 [1], the Figure 6.9.3-1: "Data Collection & Distribution for Event Notifications (Subscribe/Notify)" shows how the data can be transferred via Messaging Framework from data sources to data consumer.

Since the Messaging Framework is not expected to be standardized by 3GPP, it may not be trusted.

As concluded in clause 8 in TR 23.900-71 [1], Data Collection Coordination Function (DCCF) and Data Repository Function (DRF) and the related interfaces (interfaces between 3GPP entities and the adaptors) are to be standardized.

The DCCF and the Messaging Framework decouple the data collection between the data consumer and the data source; however, this may induce a security problem because the data consumer cannot verify that the data from the data source is not modified by the Messaging Framework and the confidentiality of the data cannot be guaranteed by the Messaging Framework.

#### 5.1.4.2 Threats

An attacker may eavesdrop or manipulate or replay the communication or initiate the MitM attacks on the interface.

If the integrity of the data collected from the data source is not protected, then the Messaging Framework may modify the data, which results in producing wrong analytics.

If the confidentiality of the data collected from the data source is not protected, then the Messaging Framework may access the sensitive data, which may cause privacy leakage.

Replay attacks may lead to usage of same data more than once, and therefore, it may cause wrong analytic results.

#### 5.1.4.3 Potential security requirements

The transfer of the data between data source and data consumer via the messaging framework shall be confidentiality, integrity and replay protected end-to-end between data source and data consumer.

Confidentiality protection, integrity protection and replay-protection shall be supported on the new interfaces between 3GPP entities and the adaptors.

Editor's Note: It is ffs if this requirement can be fulfilled, since the task of adaptors (e.g. 3CA) is to process and format data before the data is sent as notification to the data consumer.

Editor's Note: Current understanding is that adaptors are not expected to be standardized by 3GPP. To be checked with SA2.

### 5.1.5 Key Issue #1.5: UE data collection protection at NF/NWDAF

#### 5.1.5.1 Key issue details

UEs register to 5GS and request services, e.g. the initial registration request to AMF. For fulfilling the service, but also for analytics purposes, 5GS NFs will collect data about the UE being served, e.g. AMF needs to maintain a mapping between SUPI and 5G-GUTI and for accounting the time window for the service used. UE related data, processed by one NF, may also need to be transferred to another NF to fulfil a service request or for analytics purposes. UE can also provide privacy sensitive data such as positioning information, user profiling info, etc to NFs, which may be transferred to NWDAF.

This KI is about NF/NWDAF collecting information about the UEs (e.g., UE mobility events, UE registration failures) from the 5G NFs (e.g., AMF, 5G RAN etc) and determines the threats and requirements for protection of data related to UE, which are collected by core NFs.

#### 5.1.5.2 Security threats

If the communication between UE and network is not confidentiality protected, then sensitive information about UEs may be leaked to unauthorized entities.

If the integrity of the data collected from UE is not protected, the analytics may not be accurate.

Replay attacks may lead to usage of same UE data more than once, and therefore, it may cause wrong analytic results.

UE related data stored in a NF or transferred between different NFs may be altered by a malicious entity. The attacker may provide false or modified information to other NFs or an analytics function such as NWDAF. For instance, the malicious entity can modify the UE information statistics or logs sent to the NWDAF.

In case of the network is not authenticated by the UE, the UE may send UE related data to an unauthorized entity, which may lead to leakage of sensitive data of the UE.

If an unauthenticated UE is sending data, it may send erroneous data to NF/NWDAF. This can compromise the efficiency, performance and output of analytics algorithms implemented in the analytics functions. If the NF/NWDAF which is receiving UE data is not properly authenticated and authorized, the sender may transfer the UE related data to an unauthorized NF or analytics function.

#### 5.1.5.3 Potential security requirements

1. UE and network shall mutually authenticate each other.

2. The communication between UE and network shall be confidentiality protected.

3. The data collected from UE shall be integrity protected.

4. Data transferred from UE to NFs and from NFs to the analytics function shall be protected against replay attacks.

5. Authorization of NFs and analytics functions to receive, send, or transfer UE related data shall be guaranteed.

## 5.2 Key issues related to detection of cyber-attacks and anomaly events by analytics function

Editor's Note: This clause is for key issues on detection of cyber-attacks and anomaly events supported by NWDAF and its related functions, specifically to define parameters provided by UE to help detect attacks and abnormal behaviours, according to the second objective of the SID.

### 5.2.1 Key Issue #2.1: Cyber-attacks detection supported by NWDAF

#### 5.2.1.1 Key issue details

NWDAF has been defined to offer automatic network analytics and alarming, with possible capabilities of artificial intelligence and machine learning to help proactively manage the 5G network. 3GPP TR 23.700-91[1] has identified the use case of NWDAF detecting cyber-attacks by monitoring events and data packets in the UE and the network, with support of machine-learning algorithms. To achieve cyber-attacks detection, the NWDAF can collaborate with UE and any other NFs to collect related data as inputs, afterwards providing alerts of anomaly events as outputs to OAM and other NFs which have subscribed to them so that they could take proper actions.

This key issue describes what kind of cyber-attacks can be detected by NWDAF. In order to mitigate the identified cyber-attacks, the data/parameters collected by NWDAF need to be studied.

The specific cyber-attacks for which an analytics function may provide detection support include but are not limited to the following examples:

**(1) MitM attacks on the radio interface:** MitM attacks or fraudulent relay nodes may modify or change messages between the UE and the RAN, resulting in failures of higher layer protocols such as NAS or the primary authentication. The NWDAF may detect MitM attacks.

**(2) DoS attacks:** 5G has high performance requirements for system capacity and data rate, improved capacity and higher data rate may lead to much higher processing capability cost for network entities, which may make some network entities (e.g. RAN, Core Network Entities) to suffer from DDoS attack. The NWDAF may also enable the detection of DDoS attacks.

#### 5.2.1.2 Security threats

Cyber-attack may not be detected by the 5G network, thus further attacks could be conducted.

Anomaly events may not be detected by the 5G network, thus further attacks could be conducted.

#### 5.2.1.3 Potential security requirements

The 5GS system shall support the operators in the detection of cyber-attacks by providing related inputs or collecting output analytics using an analytics function such as NWDAF.

Editor's Notes: The requirement may be updated according to SA2's feedback.

### 5.2.2 Key Issue #2.2: Anomalous NF behaviour detection by NWDAF

#### 5.2.2.1 Key issue details

The 5GC supports different NF deployments that could be in distributed or redundant fashion so that the NF provides the services from several locations and several execution instances. When these NFs are distributed across multiple cloud infrastructures, it is possible that the NFs may behave in an undefined manner. The undefined behaviour of the NF may be caused by internal errors such as configuration mistakes or internal data corruption. This misbehaviour may impact one or more UE services based on the type of NF. Thus, the correlation of which NF is handling which UE data is an important aspect, such that NWDF is enabled to conclude from UE related data reported, which NF may have anomalous behaviour.

In all such instances, it is imperative that an analytics function such as NWDAF monitors the behaviour of all the NFs and ensures that the NFs behave as defined. If the NFs behave erroneously, it should be possible to detect the anomaly so that appropriate steps can be taken, e.g. by an operator, to control the potentially damaging behaviour.

Note, it is up to the operator to define the details of what NFs should report if such monitoring and detection by NWDAF is wished. However, there is a need to enable NWDAFs to receive or request reports by NFs which serve the detection of anomalous NF behaviour.

#### 5.2.2.2 Security threats

Different NFs may behave in an undefined manner. Anomalous or malicious NF behaviour could be, for instance, to try to access NF/NF service which was not authorized to a NF as NF/NF service consumer, to consume lots of resource for NF as either NF/NF service consumer or producer, to trigger DoS attack on NF service producer by continuously sending some malicious message, e.g. ill http request, etc., to try to exhaust connections of http server.

This can be either due to internal data corruption, configuration errors, or due to cross communication between NFs from different vendors. Based on the NF type, such NFs could cause damage to either one or multiple UEs. For example, in case of an AMF or SMF dedicated to a network slice, the service for all UEs within the whole network slice could be affected. Even the whole network slice could get out of service.

An erroneous NF may succeed in knocking the whole network out of service by sending wrong messages to other NFs, causing other NFs to get out of service.

The NFs within the 5GC are already authenticated and communicate with each other based on the authentication and authorization. If the NF is misconfigured or has internal data corruption, etc, the assumption of trust becomes invalid and causes potential threats.

#### 5.2.2.3 Potential security requirements

It should be possible for the network to detect anomalous NFs using the data collected from UE and NFs.

NOTE: By this requirement it is only assured that specific data can be collected by and/or reported to an analytics function. Which AI/ML is used is implementation specific and out of scope in 3GPP.

## 5.3 Key issues related to data transfer protection

Editor's Note: This clause is for key issues on protection of data transferring (e.g. privacy consideration) in the inter-NWDAF/NWDAF instances, according to the third objective of the SID.

### 5.3.1 Key Issue #3.1: Privacy preservation for transmitted data between multiple NWDAF instances

#### 5.3.1.1 Key issue details

In the case of Multiple NWDAF Instances, during the transfer of data/metadata/analytics output, it needs to be ensured that the privacy of the user is preserved.

It needs to be ensured that appropriate measures are taken by the sender NWDAF to protect any information which can reveal the privacy of the user, such as positioning information, user profile information etc., before sending privacy related data to another NWDAF instance. Privacy related information that has been allowed by the User for analysis should not be transferred without sufficient protection mechanism.

#### 5.3.1.2 Security threats

Information that can reveal the identity of the user can compromise privacy when transmitted unprotected.

If personal identifiable information related data is transferred without adequate measures, it provides a threat against user privacy and possibly against regulations on data protection.

Editor's Note: Description of the attacker model is FFS.

#### 5.3.1.3 Potential security requirements

Any information which can reveal the identity of the user, such as positioning information, user profile information, etc, should be securely protected before data is being shared or transferred to other NWDAF Instances.

### 5.3.2 Key Issue #3.2: Protection of UE data in transit

#### 5.3.2.1 Key issue details

The UE is providing the core network functions with data, which are reported to or requested by analytics functions. The transfer of any data between core network functions needs to be protected.

According to TS 23.288 [y] the NWDAF collects data from various data sources and provides Analytics Output to different NWDAF data consumers. In addition, according to the solutions for KI#2 "Multiple NWDAF Instances" proposed in TR 23.700-91 [x] the analytics data or the analytics output can be transferred from one NWDAF instance to another NWDAF instance.

Data in transit needs to be protected while in transfer between NWDAFs, NF to NWDAFs and NWDAF to another entity, e.g. DCCF.

This key issue addresses security for data in transit involving an analytics function.

#### 5.3.2.2 Security Threats

If data is transferred between NFs or different NWDAF Instances, a MitM (for instance a malicious SCP) can compromise data by eavesdropping or modification.

A rogue NWDAF Instance can send wrong or modified data to another NWDAF instance.

#### 5.3.2.3 Potential security requirements

Data transferred between core network functions shall be integrity, confidentiality and replay protected.

### 5.3.3 Key Issue #3.3: Ensuring restrictive transfer of ML models between authorized NWDAF instances

#### 5.3.3.1 Key issue details

In 3GPP TR 23.700-91 [1], Key Issue 19 describes trained model sharing between multiple NWDAF Instances. It has been concluded that *"Sharing of models or model meta data is limited to single vendor environments."*

Since machine learning models are trained using proprietary algorithms, and sometimes are also trained using sensitive data, securing them and ensuring restricted usage and secure transfer is paramount. Therefore, this key issue will study how to ensure that trained model sharing is only allowed among authorized NWDAF instances.

#### 5.3.3.2 Security Threats

If ML models are shared with a NF, which is not authorized, proprietary and sensitive implementation specific information may be leaked.

#### 5.3.3.3 Potential security requirements

Only authorized NWDAF instances should be allowed to consume ML models from other NWDAF instances.

# 6 Solutions

Editor's Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | | | | | | | | | |
| 1 Key issues related to securing the data provided to any type of analytics function | | | | | | 2 Key issues related to detection of cyber-attacks and anomaly events by analytics function | | | 3 Key issues related to data transfer protection | | |
|  | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.X | 2.1 | 2.2 | 2.Y | 3.1 | 3.2 | 3.Z |
| #1: UE data collection protection |  |  |  |  | X |  |  |  |  |  |  |  |
| #2: Network Analysis Framework for DDoS Attack |  |  |  |  |  |  | X |  |  |  |  |  |
| #3: Usage of current SBA mechanisms to protect data in transit |  |  |  |  |  |  |  |  |  |  | X |  |
| #4: DCCF determining if NF Service consumer is authorized to invoke a service to a Data Producer NF for data collection |  |  | X |  |  |  |  |  |  |  |  |  |
| #5: Providing the security of data via Messaging Framework |  |  |  | X |  |  |  |  |  |  |  |  |
| #6: Integrity protection of data transferred between AF and NWDAF | X |  |  |  |  |  |  |  |  |  |  |  |
| #7: Detection of anomalous NF behaviour by NWDAF |  |  |  |  |  |  |  | X |  |  |  |  |
| #8: Privacy preservation of transmitted data |  |  |  |  |  |  |  |  |  | X |  |  |

## 6.1 Solution #1: UE data collection protection

### 6.1.1 Introduction

This solution addresses KI#1.5 on UE data collection protection at NF/NWDAF

### 6.1.2 Solution details

For enhancing the 5GS to support collection and utilisation of data provided by the UE in NWDAF in order to provide input information to generate analytics information (to be consumed by other NFs) the communication between UE and NF/NWDAF needs to be secured.

In line with 5GS generic security requirements it is therefore proposed that the transfer of data between UE and NF/NWDAF related to UE data collection re-uses existing 5GS security mechanisms.

For UE data collection by NFs and NWDAF, the current NAS and AS security mechanisms for authentication, confidentiality, integrity and replay protection as described in 3GPP TS 33.501 are used.

NOTE: Whether user consent is necessary is subject of the user consent study FS\_UC3S.

For transfer of UE data to NF/NWDAF privacy requirements could apply.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Network Analysis Framework for DDoS Attack

### 6.2.1 Introduction

The solution addresses key issue #2.1: Cyber-attacks Detection supported by NWDAF.

### 6.2.2 Solution details

#### 6.2.2.1 Introduction

As depicted in clause 6.7.5 in TS 23.288 [4], the NWDAF could collect the following input data:

* Exceptions information from AF, including: IP address 5-tuple, exception ID, exception level, and exception trend.
* UE mobility information from OAM is UE location carried in MDT data.
* Network data related to UE mobility from AMF, including: UE ID, UE location, Timestamp, TAC, frequent mobility registration update.
* Service data related to UE mobility provided by AF, including: UE ID, Application ID, UE location, Timestamp.
* Service data related to UE communication provided by SMF, AF, UPF, including: UE ID, group ID, S-NSSAI, DNN, Application ID, Expected UE behaviour parameters, communication description per application (e.g. communication start, communication stop, UL data rate, DL data rate, traffic volume), TAC.

The NWDAF could output the following: Exception ID, Exception Level, Exception trend, UE characteristics, SUPI list (1..SUPImax), Ratio, Amount, Additional measurement, Confidence.

Specifically, exception ID can be “Suspicion of DDoS attack” means that the UE may trigger a DDoS attack. In this case, Additional measurement is “Victim's address (target IP address list)”. And the mitigation can be “PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.”

However, the analysis is just for DDoS attack to external AF.

DDoS attack to internal NF, e.g. RAN, Core Network should also be investigated. In order to make it more clear to capture the DDoS analysis, it is proposed a network analysis framework for DDoS attack.

#### 6.2.2.2 Network Analysis Framework for DDoS attack

The framework is depicted in table 6.2.2.2-1. In column DDoS attack, target network entity and attack method shall be clarified. In column analysis, input, output and mitigation are listed as the same way as TS 23.288 [4]. With the framework, it will be more clear how to capture attack and how to detect the DDoS attack.

Table 6.2.2.2-1 Network Analysis Framework for DDoS attack.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DDoS Attack | | Analysis | | |
| Target | Method | Input | Output | Mitigation |
| AF | DDoS using heavy UP traffic | AF: GPSI, external group ID, Exception information (IP address 5-tuple, exception ID, exception level, and exception trend), Application ID, communication description per application (communication start, communication stop, UL data rate, DL data rate, traffic volume), Expected UE Behaviour parameters  SMF: SUPI, internal group ID, Application ID  UPF: UE communication description per application (communication start, communication stop, UL data rate, DL data rate, traffic volume)  AMF: TAC | DDoS to AF | PCF may request SMF to release the PDU session.  SMF may release the PDU session and apply SM back-off timer. |
| RAN | DDoS using heavy RRC signaling | OAM: Global RAN Node ID, time stamp, SUPI, initial RRC message number  AMF: Global RAN Node ID, time stamp, SUPI, initial NAS message number | DDoS to RAN  Victim RAN Node ID  Malicious SUPI | AMF may provide AMF UE N2AP ID and RAN UE N2AP ID to RAN of malicious SUPI.  RAN may treat the malicious UEs based on local policy, e.g. release its resource. |
| AMF | DDoS using heavy NAS signaling | OAM: Global RAN Node ID, time stamp, SUPI, initial RRC message number  AMF: AMF instance ID, Global RAN Node ID, time stamp, SUPI, initial NAS message number, initial SM message number | DDoS to AMF  Victim AMF instance ID  Malicious SUPI | AMF may treat the malicious UEs based on local policy, e.g. release its resource. |

Editor’s Note: Rational for input parameters that how to address DDoS are FFS.

Editor’s Note: Details description for input parameters are FFS.

### 6.2.3 Evaluation

TBA

## 6.3 Solution #3: Usage of current SBA mechanisms to protect data in transit

### 6.3.1 Introduction

This solution addresses KI#3.2 on protection of data in transfer.

### 6.3.2 Solution details

Any data transferred between core network functions is protected by SBA mechanisms as described in clause 13.3 and clause 13.4 of 3GPP TS 33.501 [8] for authentication and authorization of NF Service Consumer and NF Service Producer.

According to 3GPP TS 33.501 [8], clause 13.3.0, all network functions shall support mutually authenticated TLS and HTTPS. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. Thus, communication between NFs is integrity, confidentiality and replay protected.

By using an access token issued by NRF, NFs are authorized for requesting analytics from an analytics function or providing analytics data to the analytics function.

Editor's Note: End-to-end integrity and confidentiality protection is FSS.

Editor's Note: Whether the user consent of data sharing between NFs is mandatory is FFS.

### 6.3.3 Evaluation

TBD

## 6.4 Solution #4: DCCF determining if NF Service consumer is authorized to invoke a service to a Data Producer NF for data collection

### 6.4.1 Introduction

This solution addresses KI#1.3, especially the threat that based on a request from a DCCF, the Messaging Framework may provide data from a NF Service Producer to a requesting NF Service Consumer, even though the NF Service Consumer is not authorized to receive this data.

### 6.4.2 Solution details

Currently before an NF Service Consumer invokes a service of an NF Service producer, the NF Service Consumer needs to request authorization from the NRF. The NRF determines if the NF Service Consumer is authorized to use the service of the Service Producer and provides an authorization token. The NF Service Consumer uses the authorization token in the service request to the NF Service Producer and the NF Service Producer executes the service by validating the authorization token.

The above procedure will be used when the NF Service Consumer requires the service of the DCCF for data collection. In such a case the NF Service Consumer will provide an access\_token provided by the NRF in the service request to the DCCF.

NOTE: It is assumed that the NF Service Consumer relies on the DCCF to determine the Data Producer NFs for data collection.

When the DCCF receives the request for data collection, the DCCF identifies the Data Producer NF that can provide the requested data and request authorization from the NRF to invoke the services supported by the identified Data Producers in order to retrieve the data. The issue is that in the authorization request to the NRF, the NRF will not have information on the identity of the NF Service Consumer that requested the data. It is proposed to solve the issue by allowing the DCCF to include in the authorization request to the NRF the authorization token provided by the NF Service Consumer in the service request to the DCCF. In addition, to allow the NRF to verify the identity of the service consumer it is also proposed to NF Service Consumer includes a CCA token which will be used by the NRF to verify the identity of the NF Service Consumer.

Editor's Note: Authorization aspects for MF are FFS, i.e. if MF need also be authorized to receive data.

Editor's Note: The solution shall be re-visited after SA3 FS\_eSBA\_SEC SID concludes

Editor’s Note: Procedure and messages need to be aligned with SA2

The solution is shown in detail in the following section.

#### 6.4.2.1 Detailed Procedure



Figure 6.X.2-1: Service consumer authorization for DCCF selected Service Producers

1. An NF service consumer (e.g. NWDAF) discovers a DCCF to retrieve data. The NF Service consumer requests authorization from an NRF by invoking an Nnrf\_AccessToken\_Get request including the information to identify the target NF (DCCF) and the source NF.

2. The NRF authorizes the request and generates an access token as described in 3GPP TS 33.501

3. The access token (access\_token\_nwdaf) is provided to the NF service consumer.

4. The NF Service Consumer initiates an NF service request to the DCCF which includes the access\_token\_nwdaf. The NF Service Consumer also generates a Client Credentials Assertion (CCA) token (CCA\_NWDAF) as described in 3GPP TS 33.501 and includes it in the request message in order to authenticate itself towards the NRF when the request is sent via the DCCF. From NF service consumer perspective, the NF service producer is the DCCF and end point is NRF, both included in the CCA.

5. The DCCF verifies that the access\_token\_nwdaf is valid and executes the service.

6. The DCCF determines that the requested service is provided by a different NF Service Producer(s). Since the service is provided by different NF(s) the DCCF verifies that the NF Service Consumer can access (indirectly) the services provided by the identified NF Service Producer(s).

7. The DCCF requests authorization from the NRF by invoking an Nnrf\_AccessToken\_Get request including the information to identify the target NF (NF Service Producer), the source NF (DCCF) and additional authorization information by including the access\_token\_nwdaf and the CCA\_nwdaf provided by the NF Service Consumer.

For indirect communications, the DCCF may also include its own CCA, if there is SCP in between DCCF and NRF.

Editor’s Note: whether access\_token\_nwdaf is needed for authorizing the NF Service Consumer to access the data from NF Service Producers is FFS

8. The NRF determines whether the DCCF and the NF Service Consumer (based on the access\_token\_nwdaf and CCA\_nwdaf) are allowed to access the service provided by the identified NF Service Producers.

9. The NRF generates and provides an access token to the DCCF as described in TS 33.501.

10. The DCCF uses the access token to initiate an NF service to the identified NF Service Producer to retrieve the data. If the DCCF determines that the service consumer is not allowed to use the service of the data producer then the DCCF does not instruct the MF to collect data from the data producer.

11. The NF Service Producer(s) verify the access token and execute the service.

Editor’s Note: How NF Service Producer verifies the URI sent by DCCF for receiving data is FFS.

12. The NF Service Producer(s) provide requested data in the response to step 10.

13. The DCCF forwards the provided data to the NF Service Consumer in the response to step 4.

#### 6.4.3 Evaluation

TBD

## 6.5 Solution #5: Providing the Security protection of data via Messaging Framework

### 6.5.1 Introduction

This solution addresses KI#1.4 on the security of data via Messaging Framework.

TR 23.700-91 [1] defines DCCF (Data Collection Coordination Function) for efficient data collection in 5GS. The Data Management Framework for 5GC is shown in Figure 6.9.2.1-1 in [1]. When Data Collection subscription to the Data Source and the Data Collection notification to the Data Consumer are supported via a Messaging Framework, Adaptors (3CA, 3PA) supporting 3GPP services may allow Data Consumer and Data Source to interact with the Messaging Framework.

The DCCF is a control-plane function that coordinates data collection and triggers data delivery to Data Consumers. The example procedure given in the Figure 6.9.3-1 in [1] shows the how the data collection and distribution for event notifications (i.e., Subscribe/Notify) are performed. The procedure illustrates how the DCCF manages Data Sources, so data are produced only once and how the DCCF interacts with the messaging framework, so data are distributed to all subscribed Data Consumers. Data handled by the Messaging Framework is associated with an identifier.

### 6.5.2 Solution details

This solution proposes a procedure for the confidentiality, integrity, and replay protection of the transferred data against the Messaging Framework.

For the same type of data collection, the DCCF can manage an encryption key and an integrity key. The DCCF provides the keys to the data consumer and the data producer. The data producer will use the keys to encrypt the data and generating the MIC (Message Integrity Code), while the data consumer will use the key to decrypt the data and check the MIC. In such way, the data will not be revealed to the Messaging Framework and any modification of the data can be detected. In case a new Data Consumer subscribes to the same type of data where a notification procedure is already ongoing, then a key refresh procedure is carried out. In the following the term Data Tag is used similar to 23.700-91 [1], where the Data Tag includes information to identify the Data required (e.g. a set of Event ID(s) from Data Producer NF), information to identify the UE (single UE, group of UE(s) or any UE), optionally information to identify the data producer, and filtering information such as location area or time of day where data is required from.

Our solution is exemplified using the steps of the solution shown in Figure 6.5.2-1 based on the example procedure shown in Figure 6.9.3-1 in [1]. Our solution steps are marked as bold, as additional steps to this example procedure.

Figure 6.5.2-1: Protection of data sent via the messaging framework, based on Figure 6.9.3-1 from TR 23.700-91 [1].

1. Data Consumer-1 (e.g.: NWDAF-1) sends a request for data to the DCCF. The message includes the Notification Target Address. The message may indicate whether the requested data should be sent to the Notification Target Address set to Data Consumer-1 and/or to other Consumers such as Data Repository. The Notification Correlation ID of the Consumer-1 is included in the request message and is used for notifications sent to Data Consumer-1 (e.g. in step 8).

2. If the request is for UE data, the DCCF may query the UDM/NRF/BSF to determine the NF serving the UE.

3. The DCCF determines the Data Source (e.g. AMF-1) that can provide the data and checks that the requested data is not already being collected.

**If the requested data is not being collected yet, then the DCCF generates a data encryption** **key KE and a data integrity key KI. The DCCF will keep a mapping between the subscription (Identified by a Subscription ID) and the pair of keys.**

4. The DCCF controls the message bus and the adaptors so the notifications traverse the messaging framework. The subscription to the DA includes a Notification Correlation ID of the 3PA and the Notification Correlation ID for Data Consumer-1 as received in step 1. The DA may associate these with a messaging framework. The 3PA is provided with its Notification Correlation ID and the "Data Tag". The 3CA will be provided with the consumer's notification endpoint, the Notification\_Correlation\_ID of the Consumer and the "Data Tag". The 3CA may then subscribe to the "Data Tag" in the messaging framework.

**4a. The DCCF sends the subscription response to the Data Consumer-1. In the response, the DCCF provides key KE and key KI as well as a Subscription ID.**

5. The DCCF sends a subscription request to a NF producer acting as a data source. The subscription includes the notification endpoint and Notification Correlation ID of the 3PA that is acting as the receiver for these notifications.

**The request also includes key KE and a data integrity key KI**.

6. The Data Source acknowledges the request with a Subscription ID.

7. A Notification containing the Notification Correlation ID of the 3PA is sent to the 3PA after an event trigger at the Data Source. The 3PA publishes the data in the message framework. It may use "Data Tag" the associated with the Notification Correlation ID of the 3PA received in step 4.

**The data source associates the data with a Sequence Number. The data source encrypts the data using KE and protects the integrity of the data by including a MIC (Message Integrity Code). The data source computes the MIC as HASH KI (data || Sequence Number).**

8. When the data is published to the "Data Tag", the Messaging Framework makes it available to all subscribed 3CA. In this case the only subscriber is a 3CA serving consumer-1. This 3CA maps the "Data Tag" to the Notification Correlation ID of the Data Consumer received in Step 4 (which was originally provided by Data Consumer-1) and sends the notification to the notification endpoint of Data Consumer-1.

**The message also includes the Sequence number received in step 7.**

**When Data Consumer-1 receives the data, it will check the data integrity and decrypt the data.**

9. Data Consumer-2 (e.g.: NWDAF-2) sends a request for the same Data. The message may indicate whether the requested data should be sent to Data Consumer-2, and/or to other Consumers such as Data Repository. The Notification Correlation ID of Consumer-2 is included for notifications sent to Data Consumer-2.

10. The DCCF determines that the requested data is already being collected from a Data Source (e.g.: AMF-1) and retrieves 3PA ID and the Notification Correlation ID of the 3PA.

**10a.The DCCF initiates a key refresh procedure for the data as described in Figure 6.5.2.2-1.**

**10b. The DCCF sends the subscription response to the Data Consumer-2. In the response, the DCCF provides key KE and key KI as well as a Subscription ID. The keys are the same as step 4a since Data Consumer-2 requests the same data as Data Consumer-1.**

11. The DCCF sends a subscription request to the Messaging Framework indicating that there is a new subscriber of the data. The subscribe message to the DA provides the 3PA ID, the 3PA Notification Correlation ID currently in use, and the Notification Correlation ID for Data Consumer-2 as received in step 9. The DA selects the existing "Data Tag" corresponding to the 3PA information and sends the 3CA Consumer-2's notification endpoint, the Notification\_Correlation\_ID of Consumer-2 and the "Data Tag". The 3CA may then subscribe to the "Data Tag" in the messaging framework.

NOTE: The 3CA for Consumer-2 may be different or the same from 3CA for Consumer-1.

12. After an event is triggered in the data source, a Notification is sent to the 3PA and 3PA publishes the data to the corresponding "Data Tag" on the Messaging Framework.

**The confidentiality and integrity protection are done as step 7.**

13-14. When the data is published to the "Data Tag" the Messaging Framework makes it available to the subscribed 3CAs. In this case the 3CAs serving consumer-1 and consumer-2 receive the data and send the notifications to the notification endpoints of Data Consumer-1 and Data Consumer-2 using the Notification Correlation ID of Consumer-1 and Consumer-2, respectively.

**When Data Consumer-1 and Data Consumer-2 receive the data, they will check the data integrity and decrypt the data.**

**When the DCCF provides the key KE and key KI, it also maintains a timer for renewing the keys. When DCCF decides to renew the keys, it will send to the data consumer a message with the new keys associated with the Subscription ID mentioned in step 4a. When the DCCF sends the new keys to the data consumer, it put the Subscription ID mentioned in step 6 in the message.**

Editor’s Note: The procedure and messages need to be aligned with SA2.

#### 6.5.2.1 DCCF initiated key refresh procedure

Since the keys KE andKI are shared between several data consumers and data source, it is recommended to frequently change the keys either with a limited lifetime or at a change of data consumers subscribing to the events of the data.

 Figure 6.5.2.2-1: DCCF initiated key refresh

1. The DCCF receives a new subscription request from Data Consumer-2 to an existing event notification for a specific Data Tag or the keyrefresh timer for a specific Data Tag expires/reaches the value of the key lifetime. The DCCF generates fresh keys KE and KI .

2. The DCCF identifies based on the Data Tag the subscribed Data Consumer and the Data Source. The DCCF deletes the old key pairs and binds the new key pair to the involved NFs of the Data Tag.

3. The DCCF sends a Key Refresh Request to all Data Consumers and the Data Source including the Data Tag and the new keys KE and KI.

In case the DCCF would like to store data in the Data Repository Function (DRF), then the DCCF adds the DRF as a data consumer for a specific Data Tag. The DRF then can decrypt the encrypted data and store it unencrypted in the DRF (tamperproof) memory. Once a data consumer would like to read historic data of a specific Data Tag from the DRF, then it creates a corresponding Data Tag and the DCCF will add the DRF as a data source. With those scenarios, the DRF will always be able to store the data of producers and to provide them to consumers, because the DRF will always have the corresponding keys KE and KI to encrypt/decrypt the data.

Editor’s Note: How to prevent malicious data consumers to trigger unnecessary key updates is FFS.

### 6.5.3 Evaluation

TBD

## 6.6 Solution #6: Integrity protection of data transferred between AF and NWDAF

### 6.6.1 Introduction

This solution addresses KI#1.1 on integrity protection of data transferred between AF and NWDAF.

### 6.6.2 Solution details

To enhance the 5GS to support collection and utilisation of UE related data for providing the inputs to generate analytics information (to be consumed by other NFs), the communication between UE and AF/NWDAF needs to be secured.

The NWDAF interacts with the 5GC NFs and the AF using Service-based Interfaces. When the AF is located in the operator’s network, the NWDAF uses Service-Based Interface to communicate with the AF directly. When the AF is located outside the operator’s network, the NEF is used to exchange the messages between the AF and the NWDAF as defined in Rel-16.

The existing 5G security mechanism can be re-used for the transfer of UE data over the SBA interface between AF and NWDAF. For the UE data collection by AF and NWDAF, the current NAS and SBA based security mechanisms for authentication, confidentiality, integrity and replay protection as described in 3GPP TS 33.501 are used.

### 6.6.3 Evaluation

TBD

## 6.7 Solution#7: Detection of anomalous NF behaviour by NWDAF

### 6.7.1 Introduction

This solution addresses key issue #2.2.

The 5GC supports various NF deployments in order to ensure that the NF can provide services from multiple locations. These cloud platforms may be owned and operated by the PLMN operator himself or they may be run on commercial public cloud platforms. When NFs are distributed across multiple cloud infrastructures, it is possible that the NFs behave in an anomalous manner. Such anomalous behaviour can arise either due to configuration errors or internal data corruption, or due to an attack.

To allow an operator to manage its NF cloud deployment efficiently, additional security relevant log data from the NFs can be provided to the NWDAF, which can then be used to analyse and detect the root cause for an anomaly.

### 6.7.2 Solution details

The OAM or some operator defined AF may subscribe/request to the NWDAF to notify/respond when it detects an abnormal behaviour for a particular NF instance (for example excessive resource usage or consistent failure to provide its service). There can be various causes of abnormal behaviour such as an erroneous operation at a NF, an error at the side of the cloud provider where the NF is deployed, or an impending attack at a particular NF by a malicious entity in the system.

In order to analyse the root cause of the anomaly with certain degree of confidence, more information or related data can help. Thus, NWDAF requests inputs from different entities in the system (such as OAM, NRF and NFs) for detailed analysis. Security related data for analytics can also be collected by NWDAF from the NFs. The final output analytics is then sent to the OAM or the AF for adequate measures.

The procedure depicted in Figure 6.7.2-1 allows a consumer to request analytics from NWDAF for anomalous NF behaviour and its root cause.



Figure 6.7.2-1: NF anomalous behaviour analytics provided by NWDAF

1. The OAM or operator's AF sends a request/subscription to the NWDAF for NF anomalous behaviour analytics using either the *Nnwdaf\_AnalyticsInfo\_Request* or *Nnwdaf\_AnalyticsSubscription\_Subscribe* service operation.

2. If the request is authorized, and in order to provide the requested analytics, the NWDAF may subscribe to OAM services to retrieve resource usage and NF resources configuration of all targeted NF instances, following the procedure specified in clause 6.2.3.2 in TS 23.288 [1].

3a. The NWDAF subscribes to NRF to receive notification on changes, e.g., on the load and status of NF instances registered in NRF, using *Nnrf\_NFManagement\_NFStatusSubscribe* service operation for all targeted NF instances. NF instances are identified by their NF id.

3b. NRF notifies NWDAF of changes on the load and status of the requested NF instances by using *Nnrf\_NFManagement\_NFStatusNotify* service operation.

4a. The NWDAF subscribes or requests the additional security specific log info (as specified in the table 6.7.2-1) for a particular NF by invoking the *Nnf\_EventExposure\_Subscribe* service operation.

4b. The NF then notifies the NWDAF (e.g. with the complete log report) by invoking *Nnf\_EventExposure\_Notify* service operation.

5. The NWDAF derives the relevant analytics using the inputs provided by the OAM, NRF, and the NF (as specified in the table 6.7.2-2)

6. The NWDAF provides requested NF anomalous information along with the corresponding root cause (for instance a malicious NF trying to attack other NF for denial of service, or an erroneous NF unable to provide service to other NFs) using either the *Nnwdaf\_AnalyticsInfo\_Request* response or *Nnwdaf\_AnalyticsSubscription\_Subscribe* response, depending on the service used in step 1.

Table 6.7.2-1 Security specific parameters provided by NFs (NF/NRF) to assist in detection

|  |  |
| --- | --- |
| Information | Description |
| Timestamp | A time stamp associated with the service request which was sent by the NF Service Consumer to a NF Service Producer. |
| NF Service Consumer / SCP Identifier | The consumer instance or the SCP which sends the service request along with the access token to the NF Service Producer. |
| NF Service Producer Identifier | The producer instance which receives the requests and which verifies the access token received along with the requests |
| Authorization status of NF Service Consumer | Indicated if a given NF Service Consumer is authorized to receive an access token or not, as provided by NRF. |
| Access Token Authenticity | Information such as, if access token provided is for the service request it is sent, and if it is generated for the NF Service Consumer which is requesting the service. |
| Access Token Validity | Verification result, i.e. whether the access token is valid or invalid. |
| Number of requests to access a service | Number of simultaneous requests received at the NF Service Producer for a particular time window. |
| Requested Service Name | Name of the service for which the requests had been received. |
| Service Response Confirmation | Confirmation whether the NF Service Producer was able to fulfil the service requests or not. |

Table 6.7.2-2 Inputs provided to NWDAF in assisting the detection of anomalous NF

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| Security Log Data | NF | Additional security relevant log info as described in table 6.7.2-1. |
| NF Load | NRF | The load of specific NF instance(s) recorded in their NF profile as defined per TS 29.510 [2]. |
| NF resource usage | OAM | The usage of assigned virtual resources for specific NF instance(s) (e.g., mean usage of virtual CPU, memory, disk) as defined in TS 28.552 [3] clause 5.7. |

Editor's Note: Output analytics from NWDAF is FFS.

Editor's Note: Rationale about how to derive the output from the input is FFS.

### 6.7.3 Evaluation

TBD

## 6.8 Solution#8: Privacy preservation of transmitted data

Editor's Note: The solution needs to be revised to cut off the relation with user consent.

### 6.8.1 Introduction

This solution addresses key issue #3.1.

During the transfer of data/metadata/analytics-output from one NWDAF to another NWDAF, it should be ensured that any information that can reveal the identity of the user or compromise in another way the privacy of the user is protected.

Therefore, appropriate measures should be taken by the sender NWDAF to protect any information that can hamper privacy and maybe reveal the identity of the user. Some of the examples are positioning information, user profile information, etc. These information should be processed/filtered by a NWDAF before sending the data to another NWDAF.

Thus, the privacy-sensitive information has to be protected (in accordance with the regulatory requirements and the operator's policies) before being transferred to any other NWDAF.

### 6.8.2 Solution details

To protect the sensitive and private information of the user, a privacy framework is introducedBy this, different privacy rules can be applied by different operators/vendors based upon specific policies and requirements, e.g. by local policy.

The privacy rules can be stored in the home network in

* UDM/UDR if privacy is configured per subscriber, or
* NRF if privacy is generic for all the subscribers of one or several NFs.

User privacy policies and rules can be retrieved from UDM. NRF can also push this information to NFs.

Service requests related to User data need to be indicated, e.g. by an IE 'DataPurposeID'. The NF Service Consumer (i.e. requester NWDAF1 NF) needs to send this 'DataPurposeID' along with the request to the NF Service Producer (e.g. NWDAF2). Based on this IE, the NWDAF2 will process privacy related data accordingly to the specific policy or requirement valid in this operator network, before sending a service response to the requester NWDAF1.

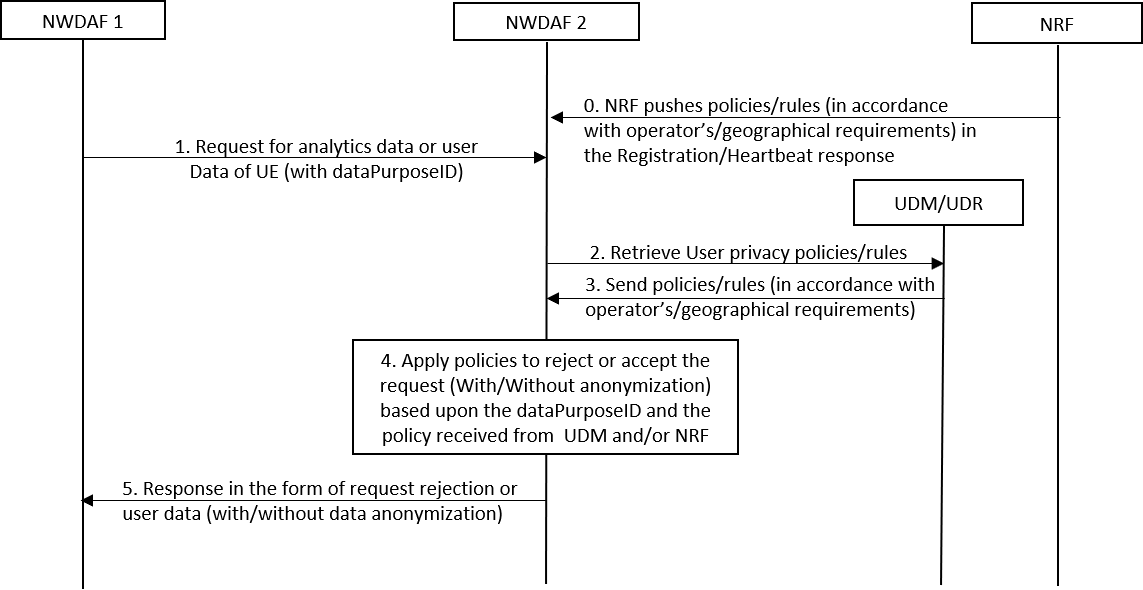


Figure 6.8.2-1: Generic Procedure to preserve user privacy based upon the predefined policies

Step 0: If an operator configures the privacy rules in the NRF (generic for all subscribers), then the NRF can push the policy/rules to NF in the response of registration/heartbeat. A heartbeat message is sent by NFs every some seconds (i.e. 10-20 seconds). Therefore whenever the privacy rule is changed in the NRF, the NRF can push updated rules to the NFs.

Editor's Note: Definition on policies/rules to be added. Clarification needed how to specify them in our TR/TS.

Step 1: NWDAF1 sends a user data request to NWDAF 2 (Sending NWDAF Instance) with an additional IE DataPurposeID indicating the purpose.

NOTE: DataPurposeID specifies the purpose of the user data request corresponding to an analytics ID. For instance, the DataPurposeID can be 'Advertisement' corresponding to the user data request of analytics ID 'location'.

Step 2: NWDAF2 sends a request to retrieve the user privacy policies for a specific subscriber from the UDM/UDR. Or it can use the locally configured policies based upon the operator's or geographical requirements.

Step 3: UDM/UDR sends the privacy policies configured for the subscriber either by the operator or by the user or based upon the privacy local policy for a specific geographical region.

Editor's Note: Clarification needed on what is privacy local policy of a specific geographical region.

Step 4: NWDAF2, after receiving the policies, applies them to the requested user data for the DataPurposeID. For instance, because of the privacy policy it can either reject the request completely or it sends the data without or with anonymization. The latter preserves the sensitive information of the user. Policies received in Step 0 are also applied along with policy received in Step 3.

Editor's Note: Clarification needed on "DataPurposeID" in relation with privacy.

Step 5: NWDAF2 sends the processed data to NWDAF1 as a response to the initial request.

### 6.8.3 Evaluation

TBD

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-10 | SA3#100bis-e | S3-202767 |  |  |  | S3-202674, S3-202766，S3-202425 | 0.1.0 |
| 2020-11 | SA3#101-e | S3-203463 |  |  |  | S3-203450, S3-203353, S3-203367, S3-203359, S3-203449, S3-203277, S3-203370, S3-203363, S3-203473 | 0.2.0 |
| 2021-01 | SA3#102-e | S3-210681 |  |  |  | S3-210569, S3-210570, S3-210581, S3-210115, S3-210571, S3-210446, S3-210109, S3-210110, S3-210572, S3-210229, S3-210573, S3-210574,S3-210679 | 0.3.0 |
| 2021-03 | SA3#102bis-e | S3-211322 |  |  |  | S3-211038, S3-211040, S3-211241, S3-211209, S3-211234, S3-211207, S3- 211201, S3-211303, S3-211239, S3- 211237, S3-211238 | 0.4.0 |